

FIG 1

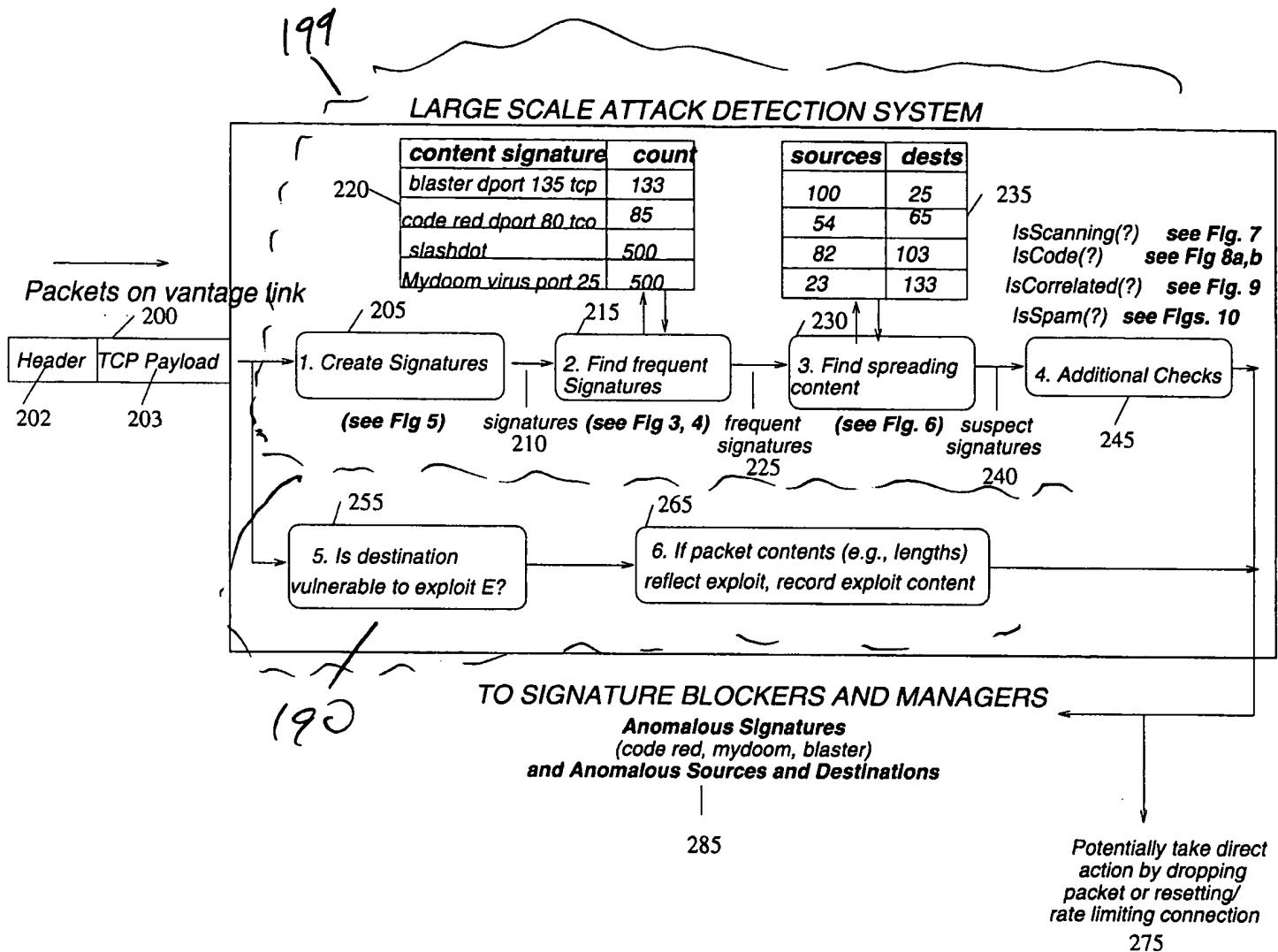


Figure 2: Large Scale Indrusion Detection System

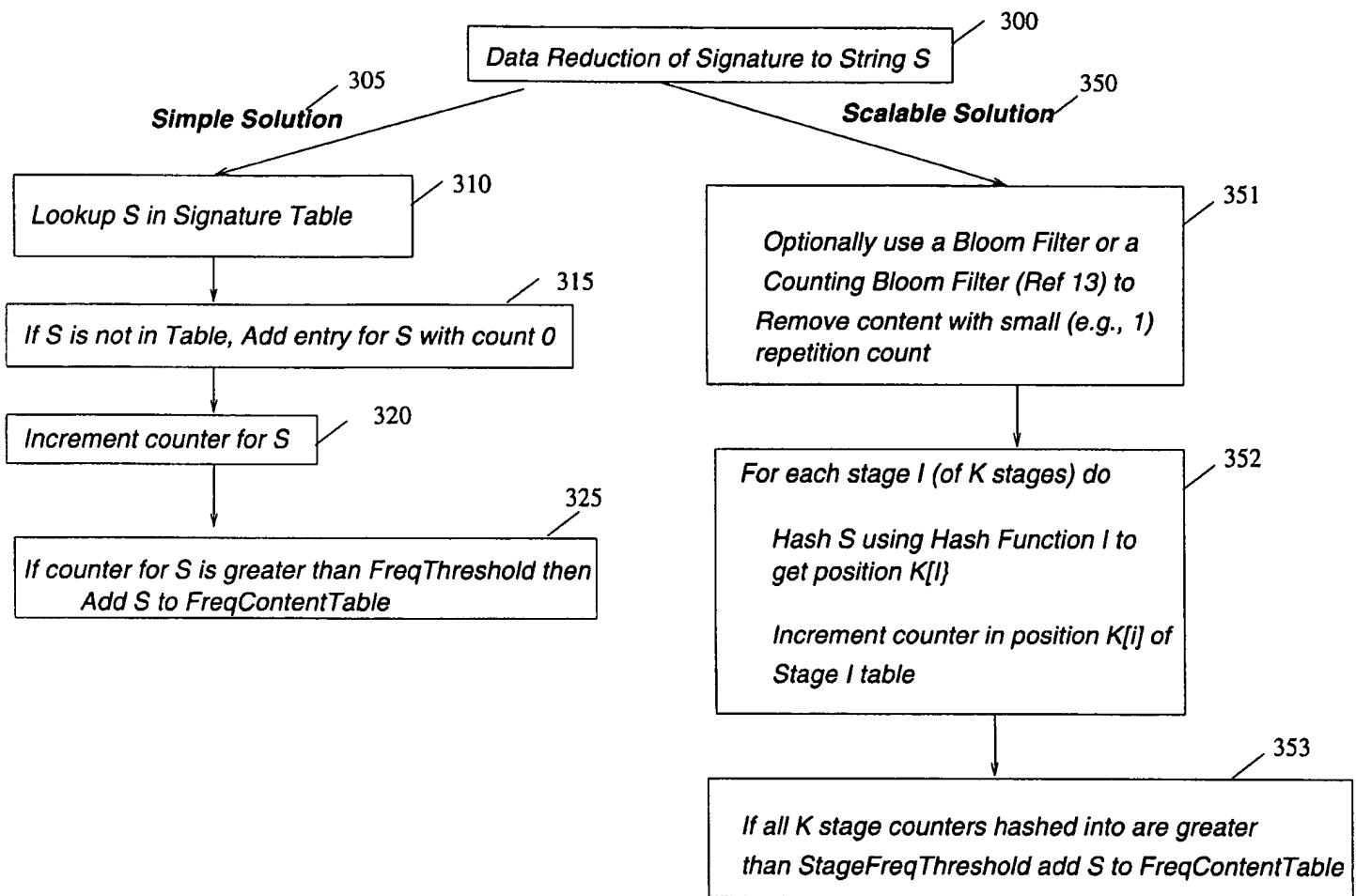


Figure 3: This figure shows the details of Block 215 of the LSIDS system of Figure 2. It sieves out frequent signatures for entry into the `FrequentContentTable`. Two alternatives are described, a simple version and a scalable version.

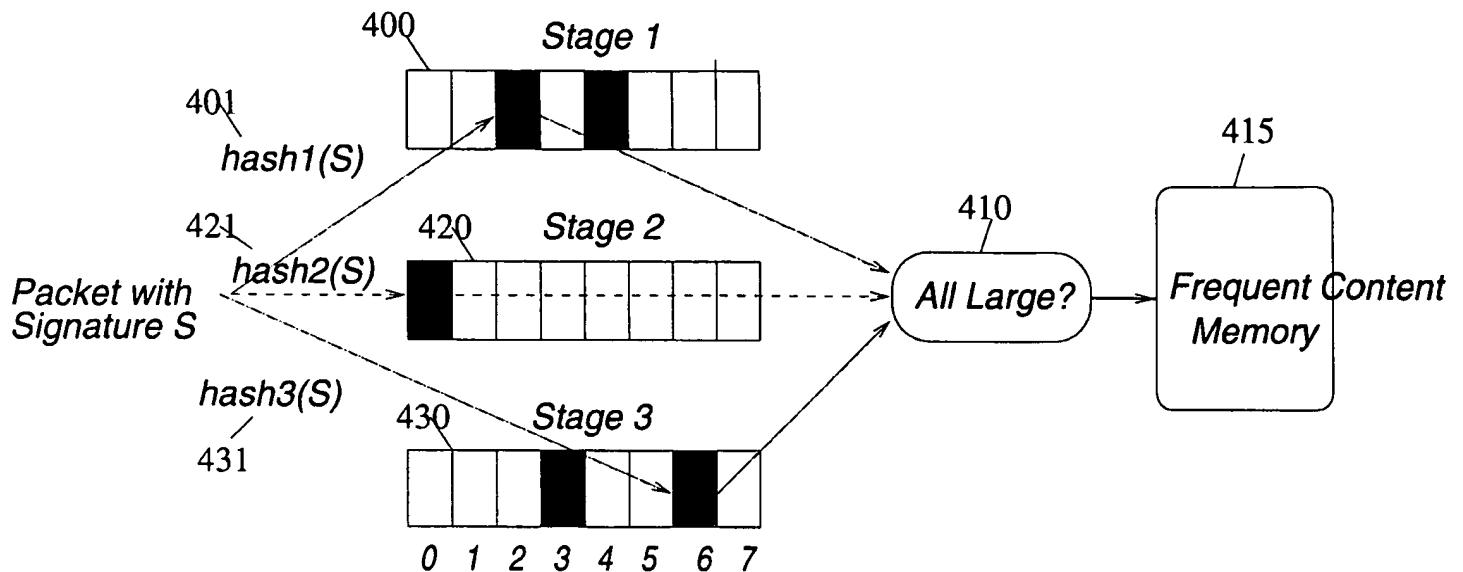


Figure 4: To identify frequent content using only a small amount of memory, a packet with content C is hashed using hash function $hash1$ into a Stage 1 hash table, $hash2$ into a Stage 2 hash table, etc. Each of the hash buckets contain a counter that is incremented by 1. If all the hash bucket counters are above the threshold (shown black), then content C is passed to the frequent content table for more careful observation.

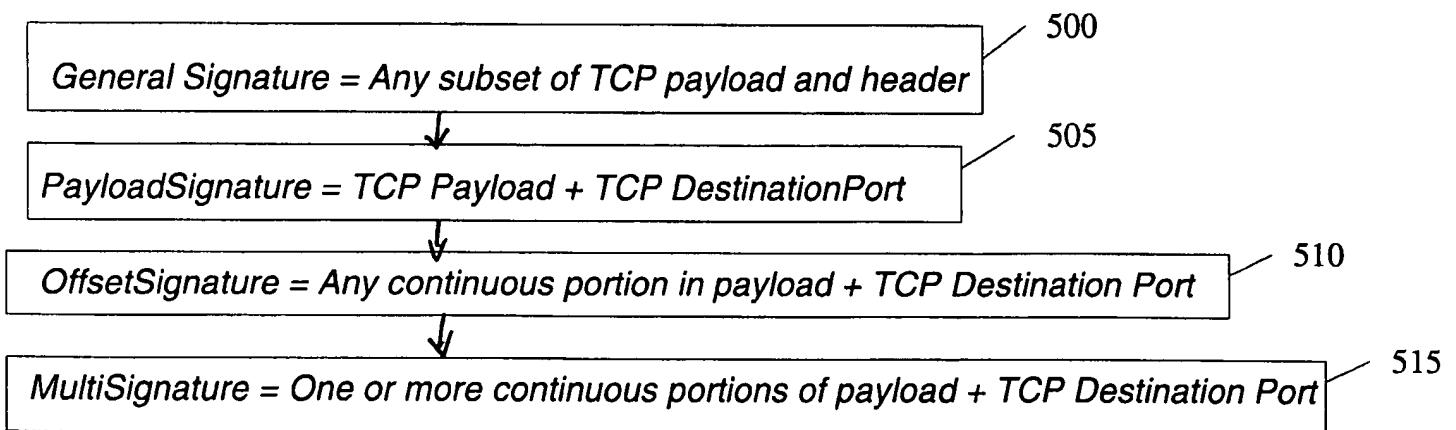


Figure 5: This figure shows the details of Block 205 of the USIDS system of Figure 2.

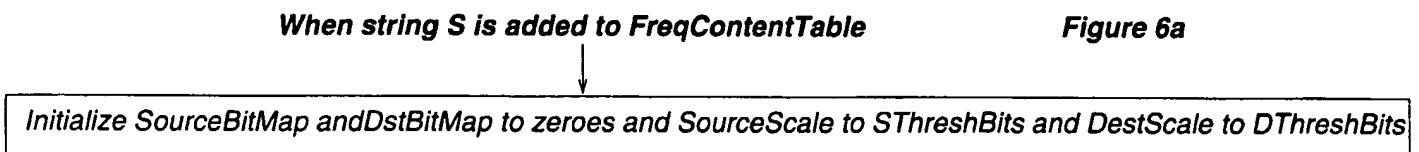


Figure 6a

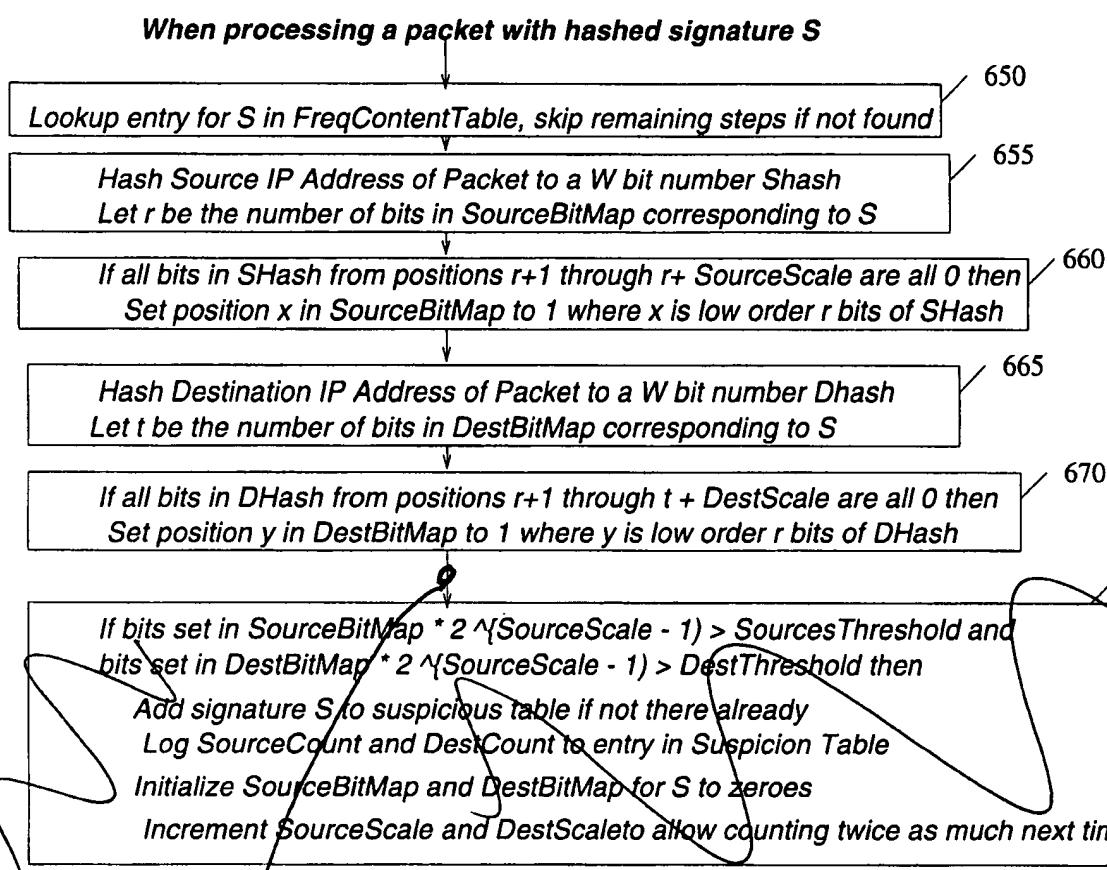


Figure 6c

Figure 6: This figure shows the details of block 230 of the LISIDS system of Figure 2. It shows how frequent signatures are checked for signs of large scale involvement and rising infection levels. Such signatures are entered in the suspicious signature table and their source count and destination counts are logged to record the progress of the infection.

scale up
by scale-factor

Form 1 bit
counting array
George Varghese et al.
15670-075001

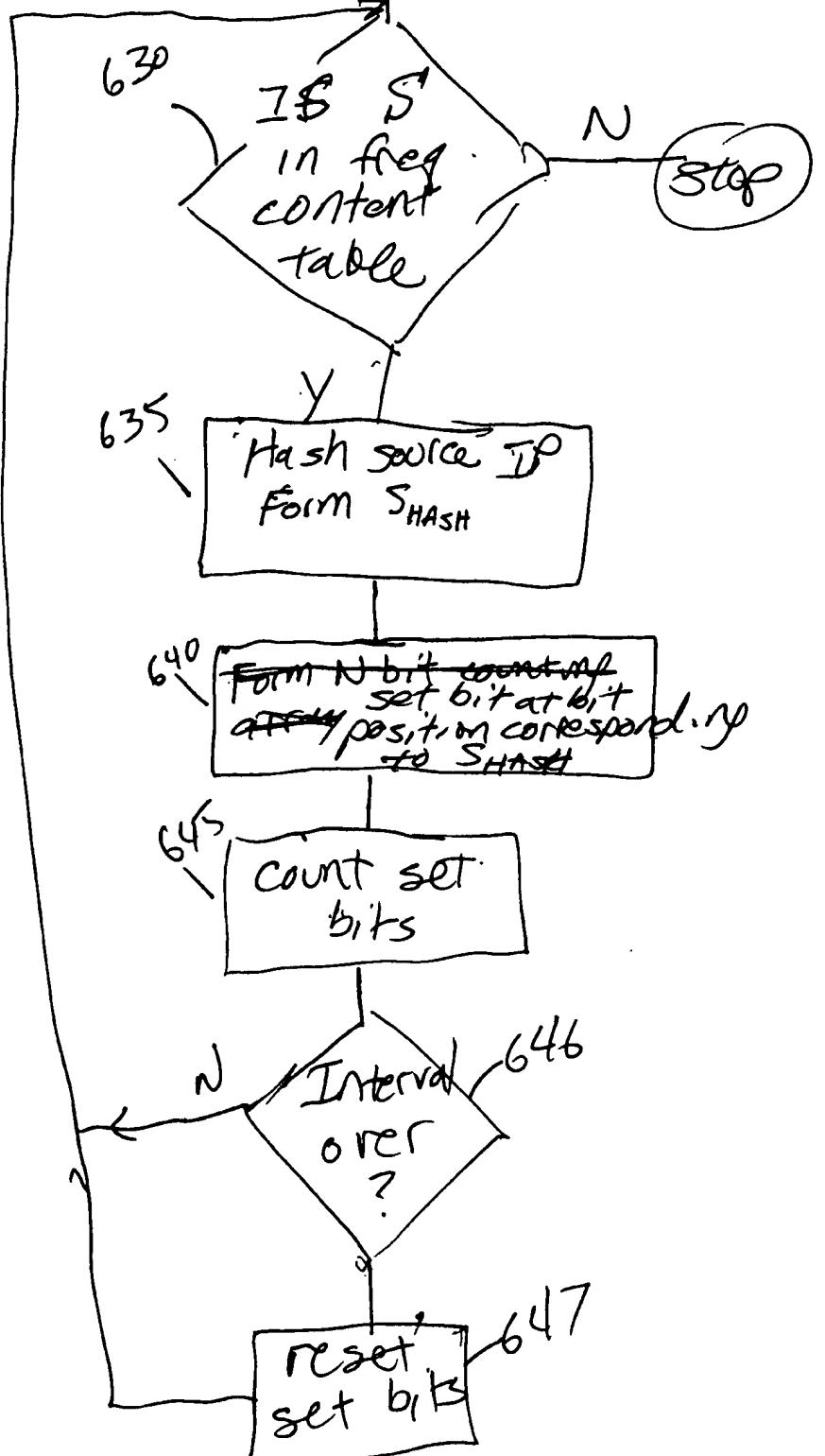
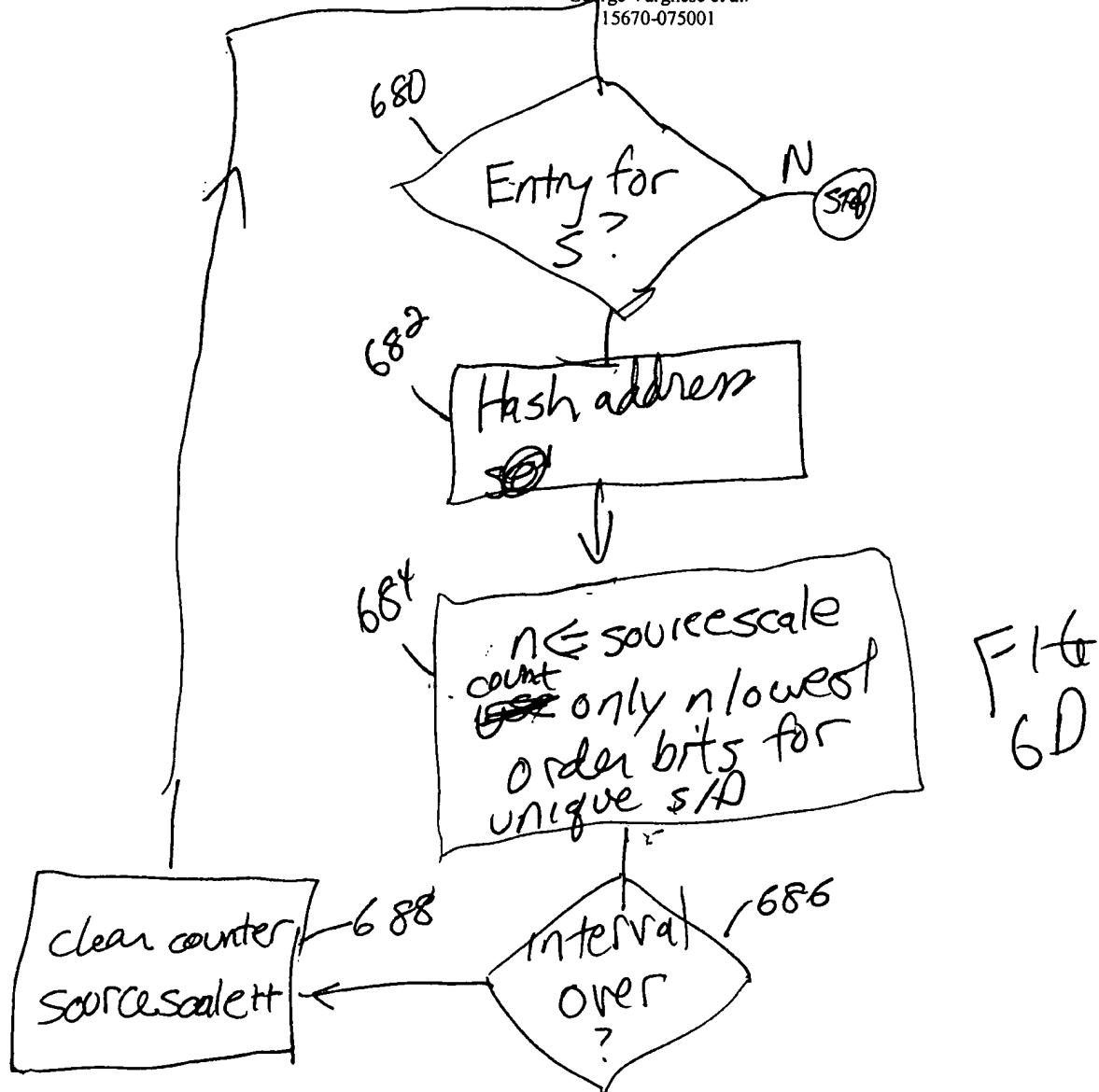


FIG
6B



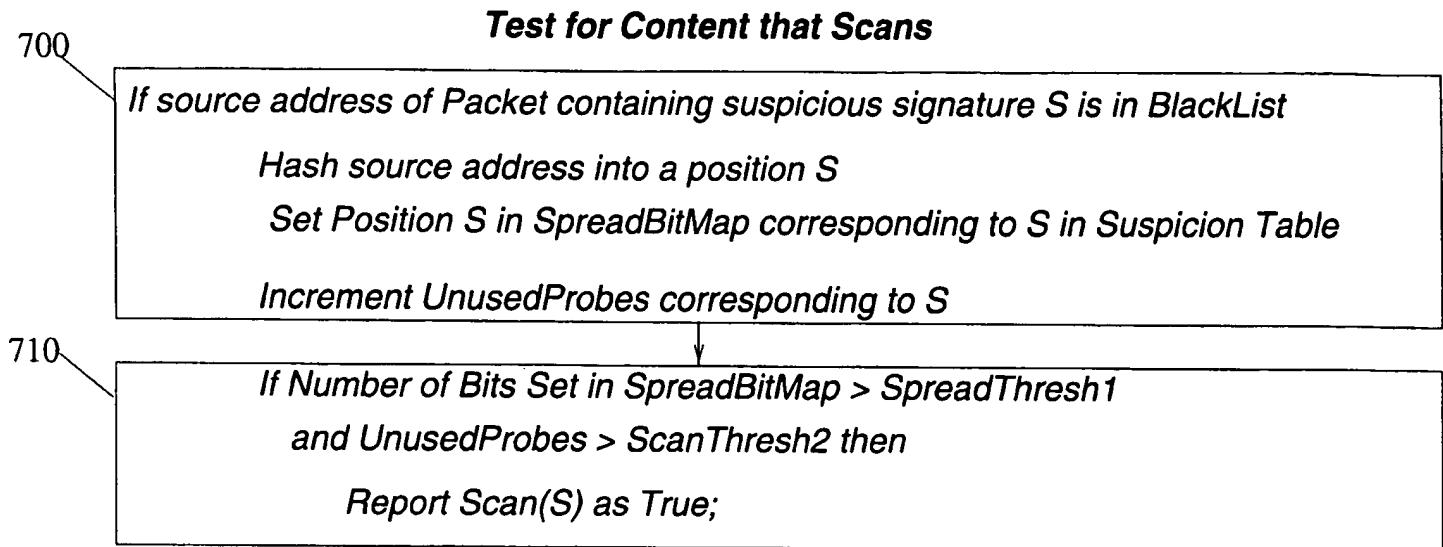


Figure 7: Scan test as part of the further tests (245) of the LSIDS system of Figure 2

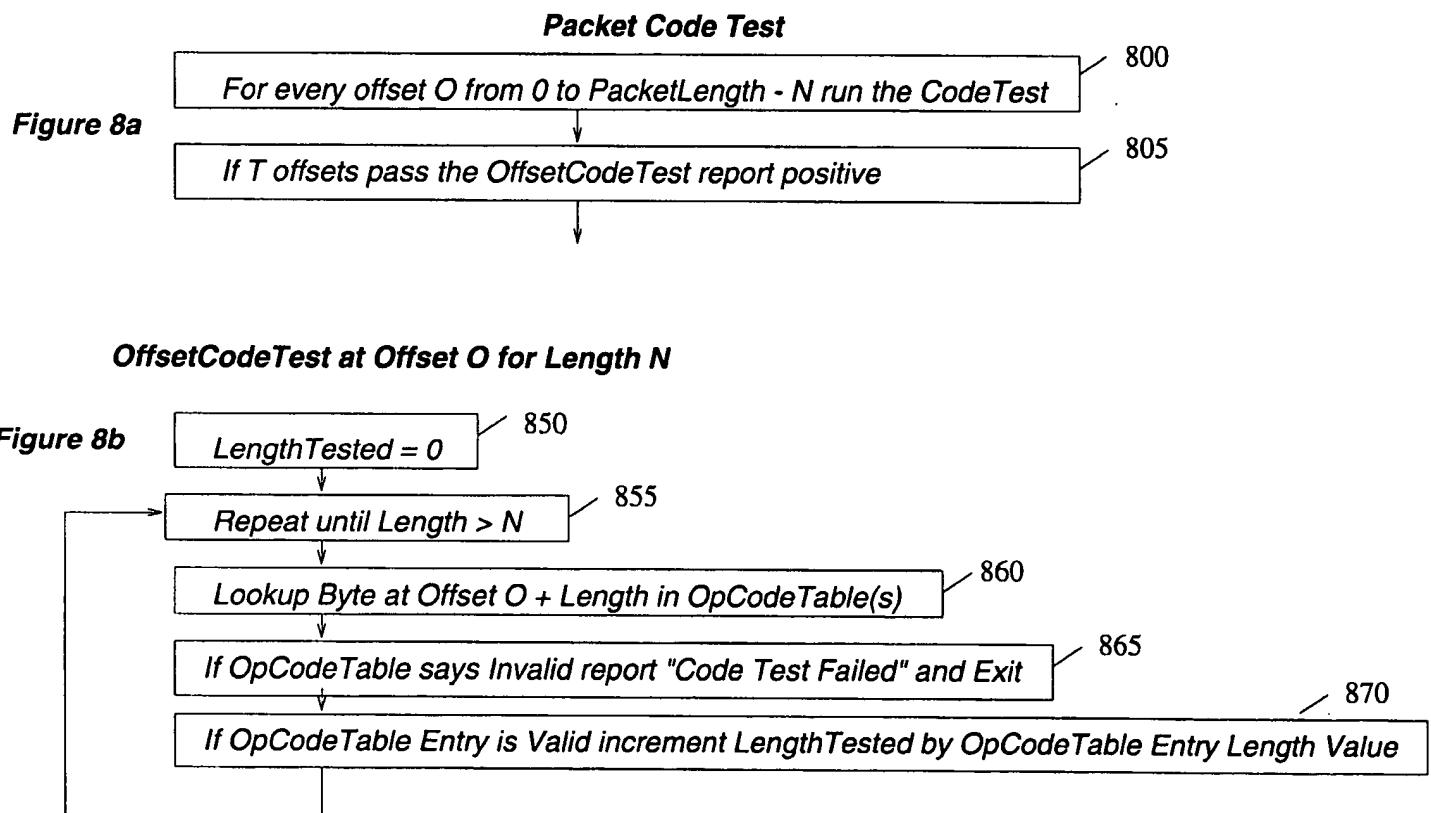


Figure 8: Code test as part of further tests (245) of the LSIDS system of Figure 2

When string S is added to FreqContentTable

905

Initialize SourceCorBitMap and DstCorBitMap to zeroes

When processing a packet with hashed signature S

710

Lookup entry for S in FreqContentTable, skip remaining steps if not found

945

Hash Source IP Address of Packet to a W bit number SHash

Let r be the number of bits in SourceCorBitMap corresponding to S

920

If all bits in SHash from positions r+1 and higher are all 0 then

Set position x in SourceCorBitMap to 1 where x is low order r bits of SHash

925

Hash Destination IP Address of Packet to a W bit number DHash

Let t be the number of bits in DestCorBitMap corresponding to S

930

If all bits in DHash from positions r+1 and higher are all 0 then

Set position y in DestCorBitMap to 1 where y is low order r bits of DHash

935

If the number of common bit positions in SrcCorBitMap for this interval and the DstCorBitMap for last interval is > CorThreshold, then S passes the correlation test

At end of interval for every suspicious signature S

110

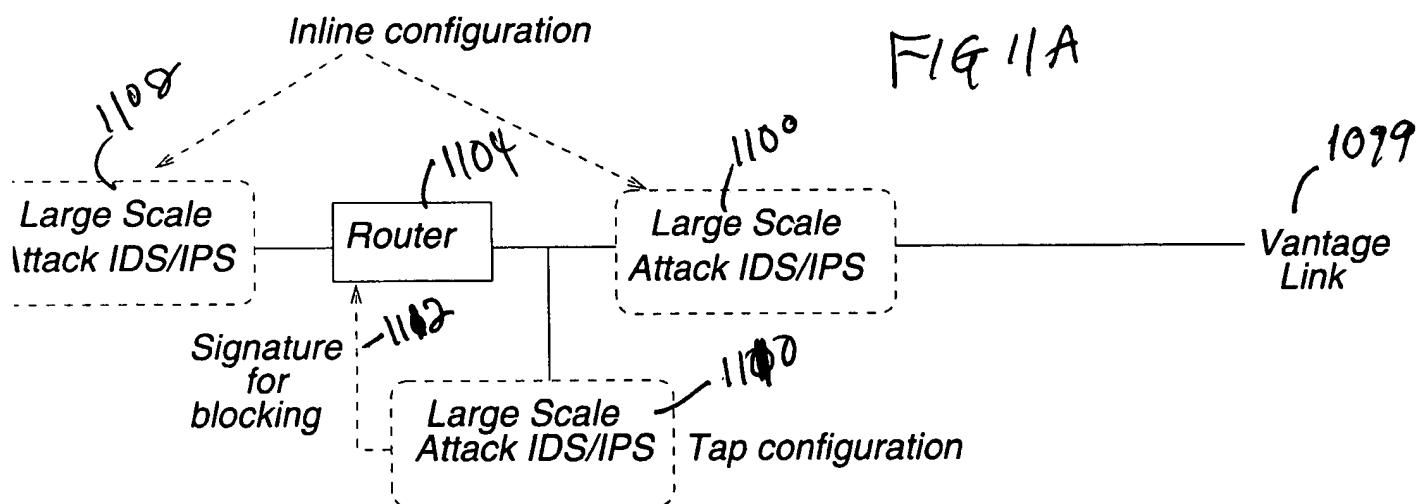
Log SrcCorBitMap and DstCorBitMap

Initialize SourceCorBitMap and DstCorBitMap to zeroes

Figure 9: Correlation test as part of the further tests (245) of the USIDS system of Figure 2

If Signature S passes a Bayesian Spam test (an example is in References) then report that S passes the spam test

Figure 10: Spam test as part of the further tests (245) of the LSIDS system of Figure 2



Sample Intrusion Detection (IDS) and Prevention (IPS) Configurations

